Published on *The National Law Review* https://www.natlawreview.com

Analysis of Attorney General Regulations to CCPA – Part 3: Verification Procedures

Article By:

Natalie A. Prescott

Overview:

The California Attorney General's draft regulations specify how businesses verify consumers' identities when they receive consumers' data requests. Specifically, Section 999.323 requires a business (i) to verify consumers' requests by using available data and implementing reasonable security measures, (ii) not to collect new data for verification unless necessary for security purposes, and (iii) to promptly delete newly collected information. Notably, a business is not required to re-identify data or to provide or delete de-identified information.

Key Elements:

- Draft Regulations, Section 999.323 (page 19) requires the business to do the following:
- Verify that the person making a request is the consumer.
- Document its own compliance with the verification requirements.
- Create a reasonable method for verification.
- Account for the possibility of spoofing, fabrication, and fraudulent requests.
- Maintain reasonable security measures to detect fraud and prevent unauthorized access.
- Employ more stringent verification for more sensitive the personal information.
- Employ more stringent verification for information that presents a greater the risk of harm to the consumer if it falls in the wrong hands.
- Match the information it already has to the one consumer provides, whenever feasible (using a vendor verification-service is permissible).
- Avoid collecting new personal information, unless absolutely necessary for verification.

- Delete new information as soon as practical, unless it is still needed for compliance with the 24-months-record-keeping requirements.

Additionally, the business should note the following requirements set forth in Section 999.324 (page 20):

- If a consumer has a password-protected account with the business, the business can use existing authentication practices, such as two-factor authentication, to verify the consumer.
- Consumers must re-authenticate themselves prior to the disclosure or deletion of data.
- If a business suspects fraud, it shall not comply with the consumer's request until further verification procedures help it determine that the request is authentic.

Finally, Section 999.325 (page 20) explains verification steps for non-accountholders. Requests by agents on behalf of the consumer are allowed, but different standards for verification apply to non-accountholders. If the consumer does not have or cannot access a password-protected account, the business must comply with both, Section 999.323 outlined above and with the additional requirements laid out in Section 999.325, below:

- The business can request that the agent match at least two data points to the information it possesses about the consumer.
- A "request to know" specific information has a higher bar for verification to a "reasonable degree of certainty" and may necessitate matching at least three data points and a signed declaration under the penalty of perjury.
- A "request to delete" specific information requires more stringent verification for more sensitive data the loss of which could be detrimental to the consumer (for example, family photos are more sensitive than browsing history).
- If a consumer uses an authorized agent to make request on their behalf, the business may require either a written permission from the consumer or direct contact between the consumer and the business.
- In short, it appears that a business can deny a request from the agent, if it deems the proof or authorization to be insufficient.
- If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and, if this is the case for all consumers whose PI the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor.
- The draft rules set forth illustrative scenarios for verifying requests to know and delete, including a situation in which a business maintains PI in a manner that is not associated with a "named actual person."

    - In that instance, a business can require the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information.

    - So, in effect, the rules appear to require that, in response to request to delete or know, a business that only associates PI with an IP address or persistent identifier would have to associate such PI with an actual name or other individual identifying information.

Takeaways:

When the business needs to verify a request from a consumer, it must first set up and then document a process for verification of the consumer's identity. The AG's solution in the proposed regulations is that the business should match the categories of information the consumer provides with the information the business already possesses. As such, the regulations advise against collecting additional information for verification, unless doing so is necessary to protect the consumer.

Businesses can also use third-party verification systems for verification purposes and do not have to provide, delete, or re-identify data that has been de-identified. Unless absolutely necessary, businesses should not collect highly sensitive information such as social security numbers, driver's license numbers, and other sensitive data. In short, the business must match the consumer's data with the data it possesses; collect new data only if necessary; implement reasonable security measures; and keep the consumers informed and safe from fraud.

Finally, consumers may rely on third-party agents to make requests on the consumers' behalf. However, businesses must then implement more stringent verification measures and have the right to refuse to cooperate with the agents if they reasonably deem the request to be unsafe, unverified, or non-compliant.

Recommendations:

We recommend the following steps, to help businesses comply with the above verification guidelines:

- De-identify as much data as possible, considering the unique needs of your business.

- For data that cannot be de-identified, create a verification mechanism that addresses the specific categories of data and how it should be used for verification.

- Train employees on how to respond to and verify consumer requests.

- Create a protocol for documenting compliance with the regulations.

- Create a protocol for and train employees on when it is appropriate to collect "new" data from the consumers, when not to collect new data, how to store it, and how to delete it in a timely manner after 24 months.

- Interview and select a vendor, if appropriate, for purposes of complying with the verification requirements.

- Exercise special care when accepting verification requests from non-accountholders.

Our next installment: Special Rules Regarding Minors

Prior installment: Business Practices for Handling Consumer Requests

National Law Review, Volumess IX, Number 291

Source URL:https://www.natlawreview.com/article/analysis-attorney-general-regulations-to-ccpa-part-3-verification-procedures